

City of Brisbane

Agenda Report

TO: Honorable Mayor and City Council

FROM: Caroline Cheng via Clay Holstine, City Manager

DATE: Meeting of February 16, 2010

SUBJECT: Web Developer Recommendation for City's New Website

CITY COUNCIL GOALS:

To develop management and fiscal systems to maximize effectiveness of city services and accountability to Brisbane taxpayers and citizens. (#11)

To encourage community involvement and participation. (#15)

PURPOSE: To have a new City website that is secure, an effective resource, and widely used by the Brisbane community.

RECOMMENDATION: Accept proposal and authorize Mayor to execute an Agreement for Professional Services (PSA) with C.J. MacDonald.

BACKGROUND:

In December 2009, the City received a federal grant, of which \$50,000 was designated towards a new website. The Public Information Subcommittee has since met on three different occasions. A summary of what took place at each meeting along with the action items taken follow:

June 9, 2009 – discussed and ranked key criteria that will be reflected in the City's Request for Proposals (RFP). Four were identified.

- Key Criteria #1: Secure Performance
- Key Criteria #2: Easy to Navigate
- Key Criteria #3: Greater Visibility of the Things Citizens are Interested In
- Key Criteria #4: Ease of Updating and Viewing Information

In addition, the Subcommittee expressed a desire to find a local web developer to ensure the new website is reflective of the town's unique and small-town spirit, and that problems could be able to be quickly addressed and patched should the need arise.

December 22, 2009 – Staff presented the Subcommittee with a recommendation for a new web developer to re-design the City’s website. C.J. MacDonald was selected based on the thoroughness of his proposal in addressing the Subcommittee’s four key criteria. Also, C.J. would be using Drupal, an open-source content management system (CMS) that is highly proficient at keeping vulnerabilities at bay. He also provided many suggestions beyond what was specified in the RFP, such as the CMS being hosted on a Virtual Private Server (VPS). This would allow for high performance, good security, and good administration.

January 12, 2010 – Staff presented the Subcommittee with monthly maintenance costs for the City’s current website and those which C.J. had determined for the new website. Albert Duro, IT Manager for the City, estimated the monthly cost for maintaining the City’s current website to be \$658.33, or \$7,900 annually. C.J.’s total monthly cost would be \$643.33, or \$7,719.96 annually.

DISCUSSION:

Should the full Council decide to accept the proposal recommending C.J. to design the City’s new website, a contract will be drafted by the City Attorney for the Mayor to sign. The contract will be based upon C.J.’s proposal (Attachment B). C.J. will be present at a later City Council meeting to show preliminary pages for the website and to answer any questions the Council may have.

FISCAL IMPACT/FINANCING ISSUES:

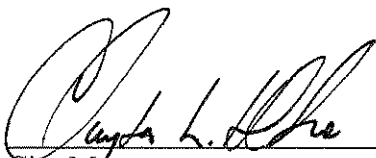
The \$50,000 grant would cover C.J.’s one time costs of \$48,200. After the website is set up, annual costs would be \$7,719.96.

MEASURE OF SUCCESS:

A secure, easily-navigable website for the City that is able to better interact with and serve the Brisbane community.



Administrative Management Analyst



City Manager

ATTACHMENTS:

- A – Staff report from June 9, 2009 Meeting
- B – C.J.’s proposal
- C – Staff report from December 22, 2009 Meeting (without attachments)
- D – Staff report from January 12, 2010 Meeting (without attachments)

City of Brisbane
Public Information Subcommittee
Agenda Report

TO: City Council via City Manager
FROM: Administrative Management Analyst
DATE: Meeting of June 9, 2009
SUBJECT: City Website Re-design

City Council Goals:

To develop management and fiscal systems to maximize effectiveness of city services and accountability to Brisbane taxpayers and citizens. (11)

To encourage community involvement and participation. (15)

Purpose:

To discuss and rank selection criteria that will be reflected in the City's Request for Proposals (RFP) when it invites contractors to bid on the design of the City's new website.

Recommendation:

For the Subcommittee to view the presentation and give direction regarding the criteria which those interested in designing a website for the City will have to meet.

Background:

At the February 17th City Council Meeting, the City Council received a staff report stating the City's current security issues, which started becoming a problem last Spring. A string of SQL injection attacks resulted in the website being kept in a perpetual "read-only" state. This makes it burdensome for the City to keep the website up to date. Prior to an update one of two staff people need to open the site for changes, then another staff person makes the changes, then site has to be closed back down. We have found if we keep the site open for changes longer than 30 minutes we become vulnerable to the SQL injection again.

Last December, the City along with Millbrae applied jointly for a federal technology grant. They received the grant, of which \$50,000 was designated towards a new website for Brisbane. The City Council agreed the next step would be for the Public Information Subcommittee to consider options and make recommendations for a web site designer developing a new website for the City.

Discussion:

In evaluating the City's website, logging onto those of other cities, and speaking with staff about their desires for the site and a web designer for information on how to improve the site, below are the key criteria which were felt to be most important when considering a web designer for the City's new website:

Key Criteria #1: Secure Performance

The City has been consulting with a web security expert, David de la Torre since last July. He proposed the City would be best off having a new website built from scratch rather than going in and trying to repair all the broken lines of code caused by multiple SQL injection attacks. In regards to the RFP, David has offered to assist the City in drafting the portion that deals with web security. C.J. Macdonald, a web design professional in town, noted that the new website should use the latest security mechanisms and be patched on a regular basis to circumvent new attack techniques.

Another item C.J. noted was that the website should be optimized for quick page load times and large files should be able to download quickly. Considering the City's current website, this could be accomplished by having more pages be HTML-based, as opposed to having to download a PDF or Word file to view the information.

Key Criteria #2: Easy to Navigate

Navigation, when done right, can be the sole reason an individual chooses to stay on a website, or leave when they couldn't find what they were looking for. In order to successfully navigate a website, one has to know where they are. One of the most common ways this is done, and which the City's current website features, is breadcrumbs. Breadcrumbs are usually located at the top of the screen and show the path the user has taken to arrive at the currently viewed page. The breadcrumbs on the City's website, however, do not serve as link anchors, with the user unable to click on them and being taken to another part of the website which may be of interest to them. Most cities do have this ability, such as the Town of Windsor. (Please see Attachment A).

Likewise, a cleaner layout for the City's departments would greatly help the user navigate, as well as give them an understanding for how our city government is structured. Currently, the navigation tree on the left-hand side of the City's website is the only way a visitor can tell where they are on the City's site. It is fairly small, with the titles of the drill-down pages forced to be very close together, thus making it difficult to read the various section titles (please see Attachment B). Other cities, such as Palo Alto, enlist the use of graphics, completely removing navigation trees from their website

altogether. (Please see Attachment B). The City of Newport Beach has chosen to show their organization chart when “Departments” is clicked on from their homepage (please see Attachment C). This gives the user a very clear visual of their city’s departmental layout, presenting the information in a way they may already be familiar with from their own work environments. From the organization chart, the visitor can click on any of the departments to learn more about them, as well as be provided with contact information of staff in case they would like to reach them specifically (please see Attachment C).

Key Criteria #3: Greater Visibility of the Things Citizens are Interested In

With the City having been able to accept credit card payments for the past four years, the items for which residents can pay using their credit card, such as water bills, business license and building permit fees, and slip rentals at the Marina, should be clearly visible from the City’s homepage. The City of Burlingame has designed their homepage to have a “I Want to...” column, with one of them being “Pay...”. (Please see Attachment E). Also, since individuals are able to register for Parks & Recreation classes and programs completely online, the fact indicating the ability to do so should be clearly identifiable on the City’s homepage.

During times of emergency, citizens will oftentimes turn to their city’s website expecting the latest, most up-to-date information from the city. A simplified version of this was seen on the Town of Windsor’s website. An emergency alert light is always displayed on the homepage, and will either be red, should the town want to notify its constituents of an emergency taking place, or green when there are no current emergencies. (Please see Attachment E).

Since the launch of the City’s current website, there has been a tremendous amount of material added to the website having to do with sustainability. Since the City holds itself as being “environmentally-progressive”, having adopted that as one of its values, a section dedicated to this effort should be a part of the website redesign. Included in this section would be announcement about upcoming “green” events such as Habitat Restoration Day, news from the Open Space & Ecology Committee, and files that demonstrate the City’s commitment to sustainability, such as a link to the City’s Green Building Ordinance. With the buildout of the Baylands, having a section similar to the City of Albany’s “Green Albany”, will be essential. (Please see Attachment F).

Key Criteria #4: Ease of Updating and Viewing Information / Events Calendar

An easy-to-use Content Management System (CMS) would allow departments to easily update their own information, without having to know HTML. Currently, the City’s website has a lot of “static” pages, which can only be changed by the City’s current contracted web designer. For instance, the navigation tree and links on the homepage’s right-hand side are not able to be updated or changed by staff. This impinges on the ease and frequency web updates are made, resulting in the website looking less dynamic than it potentially could.

Information needs to be constantly updated for users to return to a website. One of the most-frequently updated items on the website is the Events Calendar. The City's Events Calendar, however, is very small and does not reveal a lot of information at the onset. One has to do some digging, selecting the item they want to view upcoming events for. (Please see Attachment G). On the other hand, the calendar found on the City of Mountain View's website allows one to check off all the areas they want to view upcoming events of, as well as select how they would like to view the information: by day, week, month, or year (our calendar allows only "List" or "Month" view). Those viewing the calendar are able to quickly get a hold of the information they desire, increasing the possibility they will attend and get involved in community events and meetings.

Going along this line, civic participation and transparency would be a natural result of a website interested in receiving collective feedback from its users. C.J. made the comment that as much as is practical and reasonable, the website should allow and encourage civic participation with modern web 2.0 social networking tools like forums, polls, and commenting. Commenting and polling have already been implemented on the City's blog, but additional opportunities for the public to provide their input, suggestions, and recommendations would help to ensure the website is meeting the expectations and interests of the community and all who log on to the Brisbane website.

Fiscal Impact:

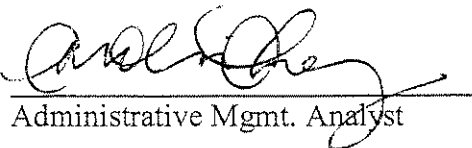
None, due to the City having received a federal technology grant.

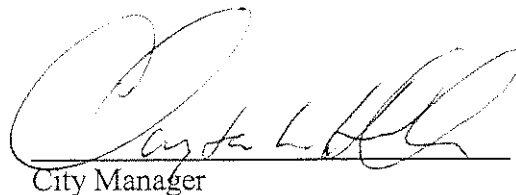
Measure of Success:

A secure, easily-navigable new website for the City that is able to better serve and inform all visitors to the site.

Attachments:

- A – Key Criteria #2: Easy to Navigate Pages
- B – Key Criteria #2: Easy to Navigate Pages (cont.)
- C – Key Criteria #2: Easy to Navigate Pages (cont.)
- D – Key Criteria #3: Greater Visibility for the Things Citizens are Interested In
- E – Key Criteria #3: Greater Visibility for the Things Citizens are Interested In (cont.)
- F – Key Criteria #4: Ease of Updating and Viewing Information / Events Calendar


Administrative Mgmt. Analyst


City Manager

ATTACHMENT B

Aloft Consulting

Website Proposal for
The City of Brisbane

C.J. MacDonald
Phone: 415-283-7237
Email: cjm@aloftcorp.com
Website: www.aloftcorp.com

City of Brisbane Website Proposal

Technology to help the administration
serve the community better

V1

Sept 25, 2009

Table of Contents

BACKGROUND.....	1
GOALS OF THIS DOCUMENT	1
Architectural Framework.....	1
Branding and Design Strategy.....	2
CURRENT WEBSITE ANALYSIS.....	3
Current Site is Inflexible.....	3
WEBSITE GOALS.....	4
Encourage Interaction.....	4
WEBSITE CRITERIA.....	5
Security.....	5
1. The Technology and The System.....	6
2. People & Services.....	7
2. The Plan.....	8
Features Requested.....	8
PRICING ESTIMATE.....	11
MAINTENANCE	12
EXPERIENCE AND QUALIFICATIONS.....	12
PORTFOLIO.....	13
Marlin Developer Community.....	13
Open Architecture Network.....	14
Aloft Corporation.....	14
CineGoGo.....	15

Ron Davis & Company	15
Kuhel Design	15

RECCOMENDATIONS16

APPENDIX A – DRUPAL AND APACHE WEB SITE SECURITY CHECKLIST17

Top Ten Vulnerabilities by Likelihood	17
Top Ten Hacker Goals	17
Basic Apache Settings.....	18
Restrict files listed.....	18
Disable Apache's directory listings	18
Restrict Drupal's file upload lists.....	18
Beware Drupal file manager-style modules	18
Restrict the files PHP scripts can access.....	18
Limit PHP file access to specific directories.....	19
Restrict the types of files served	19
Block Apache from serving hidden files.....	19
Restrict Apache to only serve files with safe file types.....	19
Restrict Drupal file uploads to only accept files with safe file types	19
Restrict the context in which files are served	19
Restrict the PHP scripts executed	20
Allow access to Drupal's "cron.php" from trusted hosts only.....	20
Allow access to Drupal's "install.php" and "update.php" from trusted hosts only ...	20
Redirect access to unallowed Drupal files to 404 "Not Found" errors.....	20
Reducing Information That can Help Hackers	21
Reduce published software names and version numbers.....	21
Disable or restrict Apache server information pages	21
Restrict Apache server status pages	21
Disable PHP information in HTTP messages	21
Disable the Apache server signature.....	21
Change the default name of the PHP session cookie	21
Remove pages that display "phpinfo()".....	21
Remove content that shouldn't be served	21
Block Apache from serving its manual	22
Move Drupal's text files	22
Move Drupal's script files	22
Move Drupal's "install.php"	22
Remove extra entries from Drupal's "robots.txt".....	22
Remove Drupal's version number from "robots.txt"	22
Remove Drupal's version numbers in CSS files or enable CSS aggregation	22
Remove Drupal's version numbers in Javascript files or enable CSS aggregation ...	22
Remove content that announces what software we use.....	22
Remove "badge" images and configuration bragging	22
Use a custom favicon instead of Drupal's favicon.....	22
Disable error and debugging information	23
Disable PHP on-page errors	23

Disable Drupal's on-page errors	23
Disable Drupal's devel module	23
Disable Apache TRACE responses.....	23
 Drupal configuration changes that limit who can post content to the site and who can view it	 23
Lock down Drupal accounts	23
Disable Drupal's anonymous user account creation.....	23
Block logins to generic Drupal accounts.....	23
Create Drupal user roles.....	23
Assign users their user roles	24
Set Drupal user role permissions.....	24
Set up SSL for Drupal logins	24
 Restrict the content users can create.....	 24
Create a safe filtered input format for Drupal's anonymous users	24
Create a safe filtered input format for Drupal's trusted users.....	24
Restrict access to Drupal's unfiltered input formats.....	24
Install a spam filter module in Drupal	24
Restrict access to PHP code fields	25
Restrict the nodes listed	25
Restrict views to only show published nodes.....	25
Restrict views to only show non-administrative nodes.....	25
Restrict access to administrator views	25
Block listing administrative vocabularies in the public site map	25
Block listing administrative vocabularies in taxonomy views	25
Restrict the nodes indexed and shown in a search.....	25
Block listing administrative nodes in the XML site map.....	26
Restrict access via Drupal search	26
Restrict the content users can view	26
Restrict access to specific Drupal nodes and content types.....	26
Restrict access to specific Drupal menus.....	26
Restrict access to specific Drupal blocks	26



City Of Brisbane Website Proposal

Background

The City of Brisbane is seeking a comprehensive assessment/analysis of the City's current website (www.ci.brisbane.ca.us) and a proposal for a redesign consistent with the objectives in the RFP filed in August, 2009

Aloft Corporation, a Brisbane CA based business doing web development work since 2004, hereby submits this proposal for consideration.

Goals of this Document

Architectural Framework

This proposal will suggest that the city use a modern, standardized, robust Content Management System (CMS) with a proven track record, good security and a large installed base. To that end we are recommending that the system be implemented in Drupal (www.drupal.org). Drupal is a powerful open source CMS that is quickly becoming ubiquitous on the web. Drupal is more advanced than many other CMS's and might be the most extensible, powerful system right now. Aloft Consulting has extensive experience implementing Drupal sites.

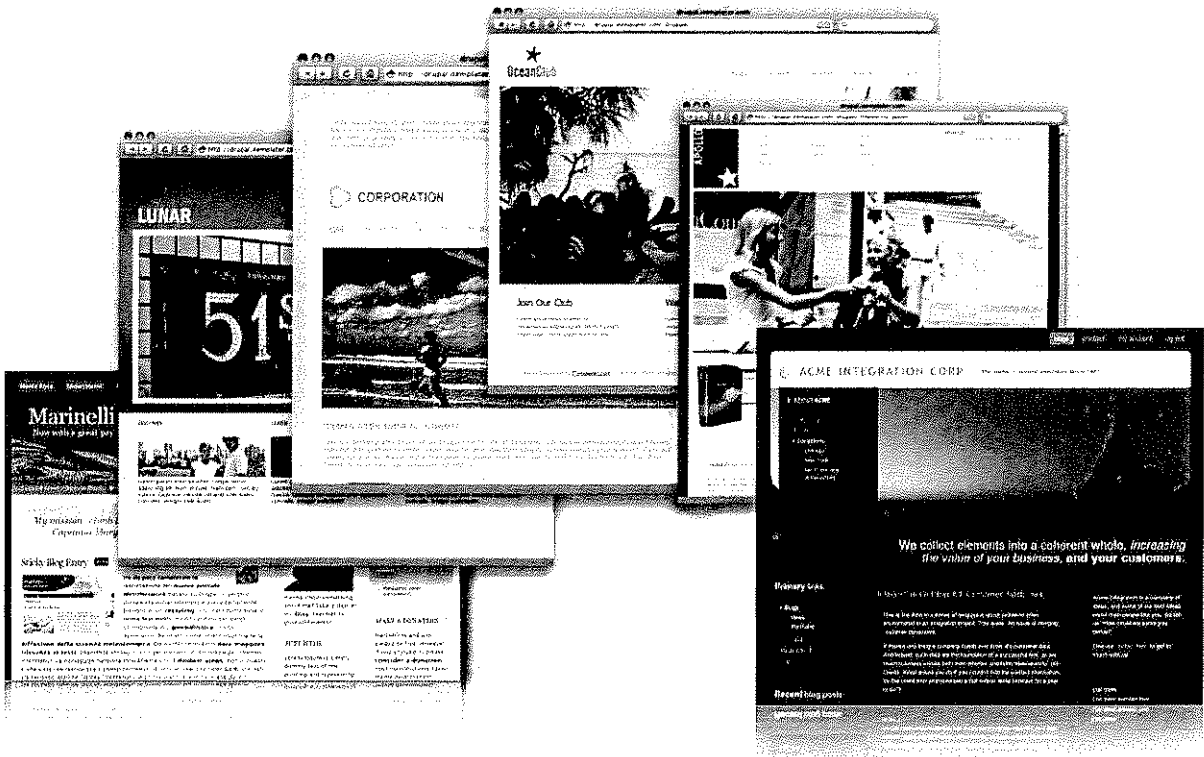
This proposal also recommends that the CMS be hosted on a Virtual Private Server (VPS). A VPS is a way to achieve many of the advantages of a private server (high performance, good security, simple administration) without the usual associated high cost and risk of hardware failure. The Hosting provider takes care of the hardware and provides other backup services. This proposal includes hosting setup and ongoing fees as part of the quote.

The VPS will be a very standard open source LAMP (Linux, Apache, MySQL, PHP) installation on CentOS (Red Hat Enterprise) and updating and patching will be included in the service contract. LAMP is well tested, high performance and high security when implemented properly.

Branding and Design Strategy

Aloft Consulting will develop a cohesive branding strategy that reflects the small town character of Brisbane. A central goal will be to make the website feel accessible - including photographs of the city from residents, as well as professional design elements, will help achieve this. The design will also be a clean, fresh look that will not become dated quickly.

The design will be image-rich, with dynamic content (an image roller on the home page, for example). The design can be based on a well-designed Drupal template that the City can choose and customize with the designer. Also, there will be a way for citizens to submit images to be moderated and posted to the home page. The blog can also be integrated into the front page itself, keeping the content current and the home page up-to-date.



Some example themes available to be chosen and customized

Current Website Analysis

Current Site is Inflexible

Proprietary system

The current website is based on a system created by the current service provider. This allows for little flexibility and has resulted in security problems.

Updates are problematic

Although the city works hard to keep the content on the website fresh, security concerns and a system that is inflexible means that the home page could use improvements. The design does not allow for handling of older items in a way that allows for access later and preserves the readability of the site.

Broken links

Related to the difficulty of updating, are links that are outdated – the “photo gallery” link goes to an external site where the photos are longer available.

Confusing navigation

The current site is lacking a logical navigational structure and does not use elements with good visual cues such as drop down menus. This is largely to be expected as the site was built several years ago, and has not been overhauled. However, the system is not flexible enough to accommodate the changes that are needed.

Lack of focus

There is nowhere for the eye to settle – all the links on the home page compete for attention and use different styles (italics, bold, colors) in a competing fashion.

Search problems

Even when it works, search gives poor results.

No easy feedback mechanism

There is not any obvious way to send in comments on the use of the site.

BRISBANE
California

SEARCH

Welcome to the City of Stars

Welcome to the City of Brisbane's Web site. We hope you find what you're looking for. Check back often, as we will update and add new information on a regular basis.

Your comments and suggestions are welcome. Please e-mail us at cityhall@ci.brisbane.ca.us

Channel 27 Live Video Streaming

A blog for the City of Stars - timely information from the City

ELECTION NEWS

Bayshore Boulevard Resurfacing Notice 9/15-9/18

Housing Element Update - City Council Review on 9/28/09

Northeast Ridge - Background Documents for HCP Compliance Hearing - Scheduled for Fall 2009 Council Meeting

Interview with PenTV on the Countywide Storm Water Pollution Prevention Program

Water Efficient Landscape Classes

Brisbane Library Historic Photo Collection

Brisbane Channel 27 Broadcast Schedule

PG&E's CARE Program

What's New in City

Recreation Class Sign-Up

City Job Openin

Community Jet Openings

City Council Age Minutes

Baylands Infor

Municipal Code

Public Works Construction Pr Updates

Public Works Pr out to Bid

BRISBANE
California

Home > Site Search

Site Search

Search function is temporary not available.

Breadcrumb trail not clickable

No images on home page

There is a little image in the corner but some large images would be nice.

File types: over-utilization of PDFs and Docs

Where possible it is better to have documents available as HTML which render faster and are more clear, as well as search better.

Video page: live only, windows media only

The city council meetings could be available in a form that would allow people to review older ones and link better to the meeting agenda and notes.

Links off-site

Some menu links (for example, fire, blog) go to external sites which makes navigation confusing. While not possible to avoid, the user should be notified that the link goes off the site.

Domain is complex and hard to remember

This proposal recommends that the City decide on a better domain name. This quote includes the purchase of a new domain such as cityofbrisbane.org. Other cities have this type of ".org" format (Palo Alto, Burlingame). Bribaneca.org or brisbanecalifornia.org are other possibilities. Note that domains are subject to availability.

Website Goals

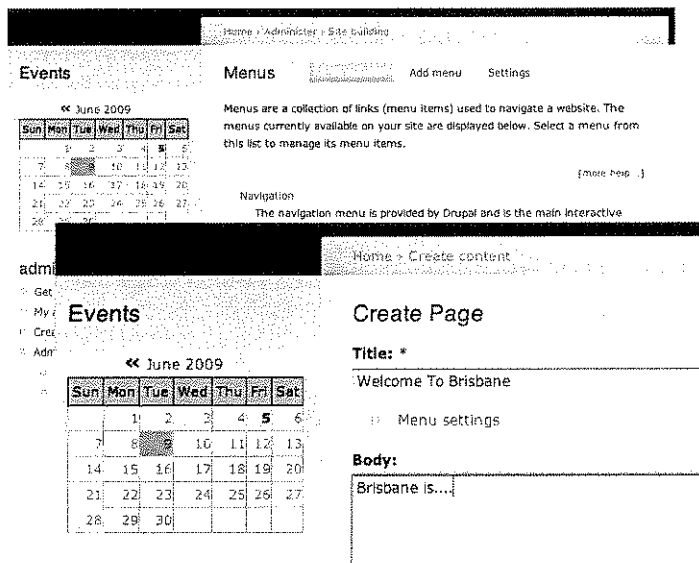
Encourage Interaction

Web 2.0 Mechanisms = Government 2.0

The new website will have a user membership process. Users, once registered will be able to do many things that are seen on social networking sites. For example, it will be possible for visitors to post comments or join groups. The extent to which the city wants this to happen is yet to be determined, and this proposal includes expert social networking consulting assistance to determine the best course of action that blends high participation with minimal risk to the city for abuse.

Organizations and Groups

It will be possible for City organizations and groups to update their pages, including



contact and description information as needed which will make their content more current. Moreover, city groups will be able to add events to the city calendar (with moderation by city staff as needed)

News

If desired, the site have an inherent blog mechanism (rather than using blogspot.com) which the city can use to post news as they do now, except that the blog will be actually on the site.

It will be possible for the city to update regular much more easily, with edit capabilities.

Calendar

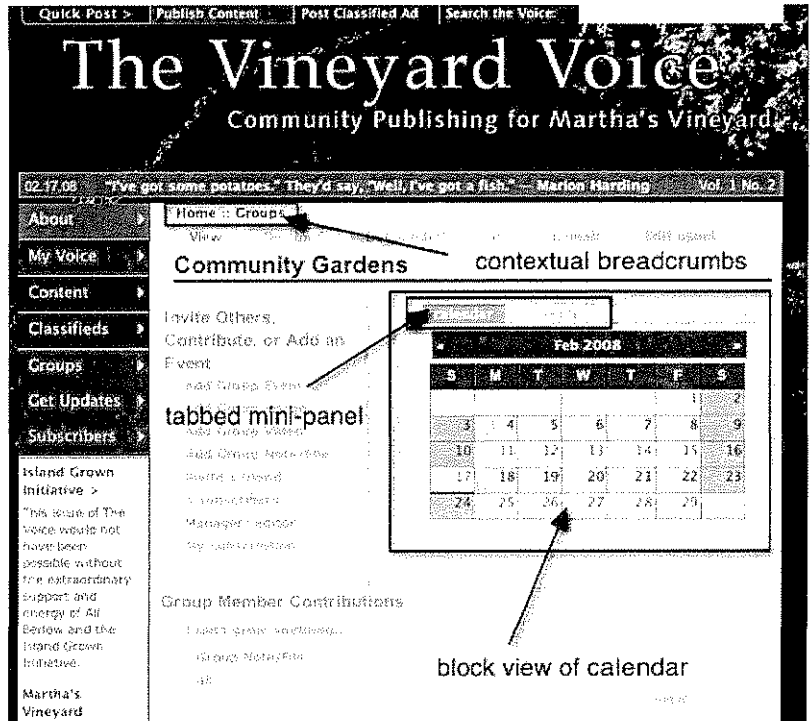
The calendar will be improved with a mechanism for groups to add their events as needed and when they have permission to do so. The calendaring functionalist will have advanced display, search and filtering capabilities, with dynamic updating functionality.

Usage Tracking

The website backend will feature some advanced reporting mechanisms on what parts of the site are being heavily used, and there will be a quarterly review and presentation of results to the city management and/or council as appropriate. These results can be used to improve the user experience by 'floating' much used pages to the top of the navigation.

Online Self-Service Options

The website will have various ways that the residents of Brisbane will be able to access material themselves. Because we are proposing an advanced CMS system, City residents will be able to add content to the site as needed. To manage this process, a revision and approval system will be developed as well as a strategy for determining what can be edited, as mentioned above.



Website Criteria

Security

The importance of security cannot be overstated. Security, however, is one of those things that is easy to talk about and hard to implement because it takes a lot of time and a lot of small steps to achieve. There are no silver bullets, and one must analyze the security of the system from the bottom to the top in a systematic approach. In

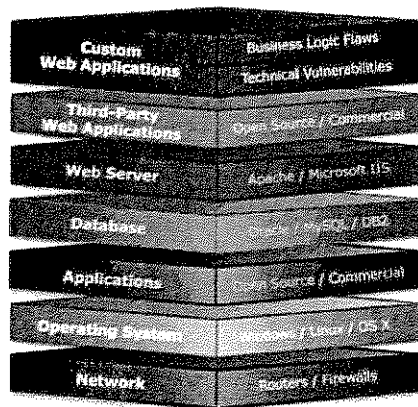
addition to having a good secure technology, one also needs multiple sets of eyes on the issue and a plan to maintain and upgrade the system. It's also important to note that there are two kinds of vulnerabilities: "well known" ones that exist at the OS and application layer, and those arising from custom code.¹ One of the main reasons we advise using Drupal is that it's a "well known" system in use on thousands of websites and watched by thousands of developers. Being open source, there are many eyes on the code and so vulnerabilities are quickly identified and patched.

There are three aspects to security covered here in this proposal:

1. The Technology and system
2. The People
3. The Plan

1. The Technology and The System

- At the network and machine layer, we use a Virtual Private Server as mentioned before, because it allows for the isolation of our system with it's own firewall. All processes are completely private to the VPS. Architecturally this is safer than shared hosting but more reliable than a dedicated machine because hardware is redundant within the grid of VPSs at the hosting provider. Moreover the server is backed up on a daily basis in its entirety. Even in the event of catastrophic failure of the host environment the server could be restored in short order. In the event that the host has a real problem where they can't be restored to, the website will be backed up on a regular basis (daily) to an external system like Amazon S3 and restoration to a new hosting provider will be possible in a few hours.
- Industry standard LAMP stack:
At the OS level we use a highly secure OS Red Hat Enterprise based CentOS Linux. Above that there is standard standard Apache, MySQL, and PHP. This system is more secure than a Microsoft system (asp.net) – by the report from White Hat Security, ASP (Microsoft) is proportionately twice as



¹ White Hat has a good security analysis which clearly outlines the security levels: http://www.whitehatsec.com/home/assets/WPstats_spring09_7th.pdf

vulnerable as PHP².

- In the middle level there is the Drupal security layer. Drupal has an auto update notification system like most modern operating systems, that is, it checks to see that its code is up to date on a regular interval (at least daily). Furthermore there are security advisories on a regular basis, to which we are subscribed and maintain several websites. An Acquia subscription will also provide access to Drupal experts and system updates as needed.
- At the top layer there is the custom code. Although custom code can be minimized with this system, modules vary in their security level. For this reason there has to be a systematic review of the less standard and customized elements of the system.

2. People & Services

In this proposal we plan to have several separate sets of people and service companies engaged in order to have several layers of overlapping attention to the security of the site:

- As the Developer, C.J. MacDonald will be responsible for the coordination of the security issues. This will involve analyzing the technology, auditing the system, explaining to the staff where the vulnerabilities are, and patching the system on a regular basis. C.J. has deep experience in Internet security; he worked for InterTrust, a media security firm for 5 years and Cenzic, a vulnerability assessment company. In addition, C.J. has experience training in information technology in Japan. He has also focused on Internet security as a consultant to a variety of clients and employers such as HotChalk, Dolby Labs and Intertrust.
- Have the hosting provider do a security audit. This is included in the quote, as is a monthly security review.
- Engage Acquia Drupal with their subscription service that allows for patch monitoring services.
- A broken link-checking module will be installed and a site uptime service will be engaged, such as Server Density.
- Hire an external Drupal security expert. We have had initial discussions with Greg Knaddison, an independent security expert who wrote the book "Cracking Drupal"³. This is also included as an estimate in the budget.

² WhiteHat Website Security Statistic Report, Spring 2009, 7th Edition, Development Technology and Vulnerabilities

http://www.whitehatsec.com/home/assets/WPstats_spring09_7th.pdf Page 6

³ <http://crackingdrupal.com/>

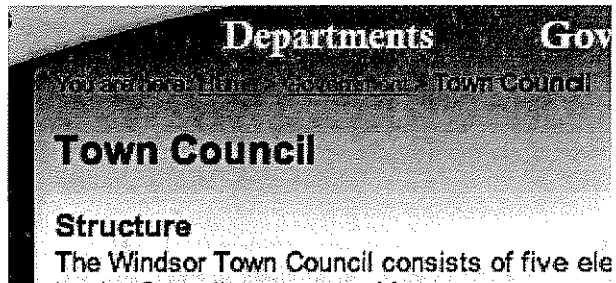
2. The Plan

When the site is installed and before it is released, audits will be done on the levels mentioned above. For a detailed description of the steps, see appendix A. Once the site is secured, we will train the relevant city staff in best security practices.

Features Requested

All of these features are included in this proposal and estimate. They have all been reviewed and can be implemented in a Drupal framework. We have included some notes on the implementation of each one, noted in **bold** below:

Hyperlinked breadcrumbs at top of page **This mechanism is available as part of the menu system in Drupal. Some tuning will be required, as well as some training for staff to know how to use this functionality when working with menus.**



Graphical layout of City departments. This can be **done with links to the appropriate section.**



ADMINISTRATIVE SERVICES



CITY ATTORNEY

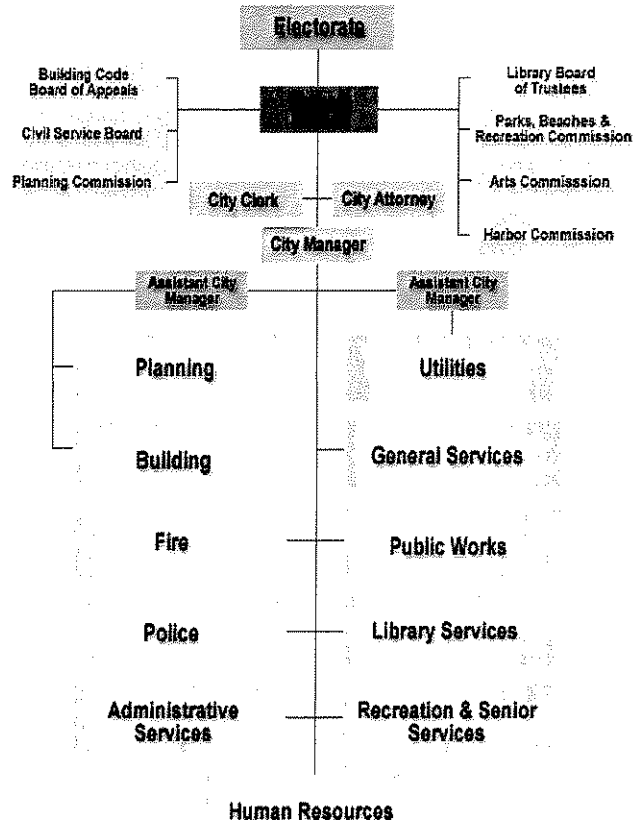


CITY MANAGER



COMMUNITY SERVICES

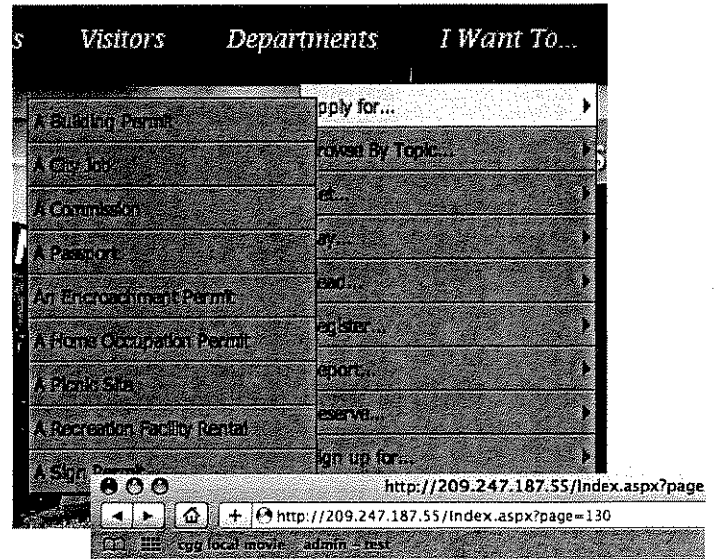
A City Organization Chart shows how departments are related to one another, with a list of departments shown in the left-hand column. **This will be done even better than the example provided, with the boxes clickable to their respective pages...**



An "I Want to..." column, listing the most-requested items at City Hall

Note that when researching this on the Burlingame site it turned up a dead link when we followed the process through to a building permit⁴. See below. This is not only a very poor user security risk since it allows hackers to find out information about the system:

This kind of user experience and security problem will be averted with the regular (daily) execution of a **dead link checker as well as log monitoring**



Citizens notified of emergencies through a red or green light on

homepage. **This will be done in such a way that it will be easily configurable from the administrative interface (not programmatic).**

Special "Green" section dedicated to environmental concerns, questions, programs, and events. **This will be done as its own section, and be easily added to by City staff.**

Rotating photos of the community and its members, with captions. **This will be done in such a way that staff will be able to easily add and change photos on the site. See www.cinegogo.net or www.aloftcorp.com to see examples of this kind of rolling slideshow.**

Bad Request (Invalid Hostname)



⁴ See either link at <http://www.burlingame.org/index.aspx?page=700>. At the time of writing, links were broken and led users to this terrible error message.

Interactive Events Calendar lets you select what meetings/events you want to see. **This will be done in a way similar to the Mountain View site, except with some UI improvements and active (AJAX based dynamic updating). Also it is possible embedded maps for the event.**



Calendar Legend
 Current Selected Date
 Day has events

JUMP TO TODAY
 September 2009
 JUMP TO MONTH

- Other
- Public Meeting
 - Special Meeting
 - City Council
 - Meet with the Mayor
 - Council Standing Committees
 - General Meetings
 - Special Meeting
 - City Task Forces
 - Environmental Sustainability Task Force

City Calendar
 Events for the week starting on Sunday

View List By: DAY WEEK MONTH YEAR
 Printable Version:

September 22, 2009 (Today)
 Tuesday

- 4:15 PM Council Appointme
- 6:00 PM City Council Meetin

September 23, 2009
 Wednesday

- 4:00 PM Administrative Zon
- 7:00 PM Development Revie

September 24, 2009
 Thursday

- 6:30 AM "Chat with MAK"
- 7:00 PM Council Neighborh

A Service Request Tracking System to receive, schedule, and follow up on citizen citizens are able to monitor **Will be done with an mechanism.**

Separate archiving of PDF documents for each department (i.e. the Office of Emergency Services currently archives information in the Public Works folder). **Implemented with several roles per requirements – each role will have the right to create and attach documents to their pages**

A better City website search engine. Google Mini, a search technology based on the same technology as the Google.com search engine may allow for improved search results. **Mini is for intranets - google search can be implemented or apache solr can be used which gives google-like results and works within the context of the site. Even google people use it -** http://news.cnet.com/8301-13505_3-10321751-16.html

Maintain a consistent look and feel through the use of content and style standards as well as some sort of consistent header, footer, or frame for every page on the website. **Achieved through the use of an advanced templating system. With some caveats, the template can be changed later to refresh the site and keep the structure the same.**

Create an archive section using recovered historic photos (with captions that have already been created) that is linked to the Brisbane History section. **Will be provided**

Utilize more Flash and make it more interactive-looking (less like a city website) **Dynamic slideshow images on the homepage, easily updated. Calls to action like links to featured groups and the blog on the home page will make this much more interesting and engaging**

PRICING ESTIMATE

These fees are all-inclusive and cover the items above.

	One time	Monthly
Setup	\$1,500	
Design	\$5,500	
Interactive (Web 2.0) strategy consulting	\$2,000	
Installation	\$2,000	
Hyperlinked breadcrumbs at top of page	\$1,100	
Graphical layout of City departments	\$1,650	
A City Organization Chart shows how departments are related to one another, with a list of departments shown in the left-hand column	\$1,800	
An "I Want to..." column, listing the most-requested items at City Hall	\$3,500	
Citizens notified of emergencies through a red or green light on homepage	\$950	
Special "Green Brisbane" section dedicated to environmental concerns, questions, programs, and events	\$1,800	
Rotating photos of the community and its members, with captions	\$3,200	
Interactive Events Calendar lets you select what meetings/events you want to see	\$4,500	
A Service Request Tracking System	\$3,500	
Separate archiving of PDF documents for each department	\$3,200	
A better City website search engine	\$2,000	
Maintain a consistent look and feel through the use of content and style standards as well as some sort of consistent header, footer, or frame for every page on the website.	Included	
Create an archive section using recovered historic photos	\$1,500	
Utilize more Flash and make it more interactive-looking (less like a city website)	\$2,500	
Training	\$3,000	As needed \$85/hr
Application later Security Audit (GVS)	\$3,000	Included

Hosting, Backups and Security		\$367.08
Core hosting fee --- Includes 1.2Ghz of CPU, 768MB RAM, 30GB Storage, 750GB/month bandwidth		Included
Monthly security audit (done by hosting provider)		Included
Daily backups		Included
Server uptime monitoring		Included
Search service and security notification service		Included
Monthly maintenance charge		\$420.00
Total	\$48,200	\$787.08

Maintenance

The contractor (C.J. MacDonald) will maintain and manage the site on the back end and be available for support as needed. 8 hours a month are included in the service contract, hours above that are billed as needed at \$85/hr.

Response time is guaranteed same or next business day, and availability is via telephone, e-mail, or instant message.

C.J. is a local Brisbane resident who lives two blocks from city hall. He is able to be onsite on very short notice to help City staff with any issues that may arise.

Experience and Qualifications

C.J. MacDonald has been a web developer for 15 years, since the earliest days of the Web. He has developed sites for businesses, schools, and individuals. He has extensive experience with dynamic website design and is a CMS architect. He has his own company based in Brisbane, Aloft Consulting, which is focused on Drupal development as well as other CMS services. His corporate website, along with his wife Jessica is available at www.aloftcorp.com

Other people on the project will be involved as needed:

George Inglis is a graphic designer with an eye for clean design.
<http://www.linkedin.com/in/georgeinglis> - He runs a design firm called propel design.
<http://www.propelidesign.ca/>

Greg Knaddsen is a Drupal security expert and will be available to do a security audit. He wrote the book "Cracking Drupal".

<http://growingventuresolutions.com/about/team>. He runs a company called Growing Venture Solutions.

VPS.net is the hosting provider and will provide a monthly security review of the site. The CEO is Detlev Bredhal - <http://www.linkedin.com/in/ditlev>

Portfolio

Marlin Developer Community

Marlin is...
the only truly interoperable and open digital content sharing platform.

Competitive
Marlin's comprehensive content sharing platform offers a simple, open, and elegant solution for powerful content services offered on a variety of devices.

- Features Profile
- Use Cases
- Download Specifications

Complete
Marlin provides the technology, the partners, and the trusted services necessary to develop and deploy end-to-end multimedia distribution systems across all networks.

- Partner Solutions
- See How Marlin Works
- White Papers & More

Growing
Backed by leading device manufacturers and licensed by technology and content partners worldwide, Marlin is in the market today and poised to transform tomorrow.

- Sony PS3 & PSP
- More Success Stories

News & Events

- Verimatrix Demonstrates Multirights DRM Interoperability with Open IPTV Forum's Marlin Standard
Sep 08, 2009, Amsterdam, EC 2009... [read more]
- Marlin After Hours Networking Event

This site makes extensive use of Drupal and features CRM integration with Salesforce as extensive use of roles and single sign on across several systems. Done for InterTrust. <http://www.marlin-community.com>

Reference: Talal Shamon, CEO, Intertrust Technologies Corporation, talal@intertrust.com, 408-772-9363

Open Architecture Network

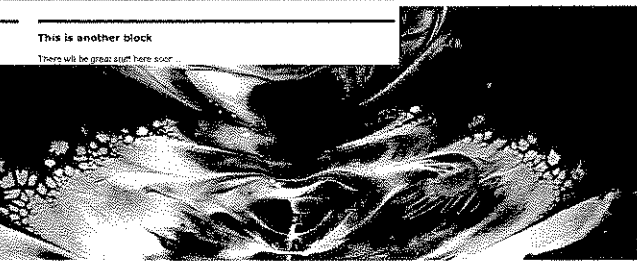
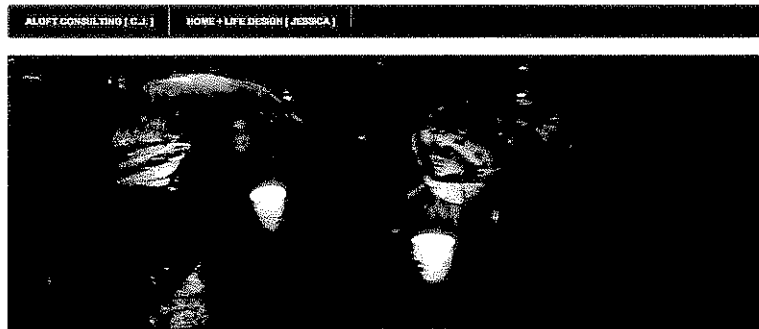


This Drupal site involved custom coding done on the Project module, and is part of the nonprofit Architecture for Humanity. www.openarchitecturenetwork.org

Reference Kate Stohr, Co-Founder kstohr@architectureforhumanity.org 646 554-7671

Aloft Corporation

ALOFT corporation



This site makes use of a dynamic slideshow on the home page
www.aloftcorp.com
 Reference: Jessica Aloft, owner
j.aloft@gmail.com
 415-657-0288

CineGoGo

CineGoGo
RUN YOUR OWN BIG-SCREEN MOVIE THEATER

 Search

HOME GET STARTED FESTIVALS MOVIES SCREENINGS

SHOPPING CART

0 Items Total: \$0.00

USER LOGIN

Username or e-mail: *

Password: *

LOGIN

- Create new account
- Request new password



SEARCH

SEARCH

RUN YOUR OWN BIG-SCREEN MOVIE THEATER!

Our online service allows anyone to create and monetize big-screen theatrical experiences anywhere - a gym, community center, school, cafe, bar, restaurant, a park or even a parking lot! All you need is a digital projector and a broadband connection.

UPCOMING FESTIVALS

SAN DIEGO FILM FESTIVAL

San Diego Film Festival

PICK A FESTIVAL MOVIE

Year:

Genre:

Film Festival

UPCOMING CINEGOGO SCREENINGS

C.J. MacDonald was the CMS architect for this site, which was all done in Drupal 6. It makes extensive use of the date and calendar functions to arrange film events, and has over 600 pages. www.cinegogo.net

Reference: Kal Deutch, Founder
kal@cinegogo.com 415-999-6226

We have also done web design and/or development in the past for local businesses and civic groups, including

Ron Davis & Company
ron@rondavis.com 415-846-3077

Kuhel Design
Jerry Keuhl kuhelsdesign@sbcglobal.net 415-215-6081

Mothers of Brisbane
Jessica Aloft j.aloft@gmail.com 415-657-0288

Reccomendations

"C.J. combines professionalism, creativity and a sense of excitement and motivation that is rare. His enthusiasm and appreciation for the people and the technology is inspiring. I would not hesitate to recommend C.J. and look forward to working with him in the future." September 15, 2009

Brent F. Barrett, VP of Production, Montreal Media
was a consultant or contractor to C.J. at Aloft Consulting

"CJ is the opposite of the "me first" people none of us likes to get stuck with on a project. He's very easy to collaborate with, and very effective off the mark - one of those rare people that within 5 minutes can grasp the essence of a project and jump right in. To do that you need smarts, knowledge insight, and listening ability - CJ has all of these. On top of that he's just an excellent guy and fun to work with."

April 5, 2008

Rob Swick, Owner, AlphaSearch
was with another company when working with C.J. at Aloft Consulting

"I enjoyed working with C.J. on what turned out to be a rather complex project. His availability and the ease of communication allowed us to meet client expectations. I highly recommend C.J. and look forward to working with him on future projects."

March 2, 2009

George Inglis, Designer, Principal, Propel Design
worked directly with C.J. at InterTrust

"CJ was very instrumental in educating me on VIA's licensing programs, particularly how various licensees implement MPEG audio technologies across the consumer electronic supply chain. His technical knowledge and ability to research issues was impressive." August 4, 2005

Jason Johnson

worked directly with C.J. at Dolby Laboratories

"C.J. is very passionate and working with him was professional. He is a great team player who brought forth the valuable knowledge needed to get done what needs to be done. He is someone you can go to for anything. He is a "down to earth" guy!

C.J. can always be counted on and I highly recommend him. I look forward to working with him on any future projects." May 5, 2009

Tyler Clasen, 3D Artist/Animator, Pandoodle Inc.

worked indirectly for C.J. at Aloft Consulting

"C.J. is a versatile, strong team player who I always call on for vital projects -- his mix of technical depth and deft touch with presenting a tight, persuasive message make him a consistent go-to guy." February 28, 2005

Alexander Mouldovan, Director, New Ventures, InterTrust

worked directly with C.J. at InterTrust Technologies Co

"C.J. was a great asset to InterTrust. He created very attractive websites and marketing material. His skill in product demonstrations and presentations certainly enhanced our position with customers and investors alike." February 15, 2005

Alan Arndt, Senior Design Engineer, InterTrust Technologies

worked with C.J. at InterTrust Technologies Co

Appendix A – Drupal and Apache Web Site Security Checklist⁵

Security is a long and continuous effort. Here is an abbreviated outline of the security checklist that will be used to achieve high security for the City of Brisbane. The good news is that a good security policy, consistently maintained, makes it very, very hard to hack the site.

Automated attack tools are widely available. Running them takes little more than a mouse click. These tools are programmed to poke at every nook and cranny of a web site, so we will configure even the obscure security settings.

In a 2009 report (PDF), White Hat Security reports that 82% of the web sites they tested had significant vulnerabilities. Using the Web Application Security Consortium's (WASC's) threat classification scheme, they estimate the top ten vulnerabilities by likelihood are:

Top Ten Vulnerabilities by Likelihood

Vulnerability	%
Cross-site scripting	65%
Information leakage	47%
Content spoofing	30%
Insufficient authorization	18%
SQL injection	17%
Predictable resource location	14%
Session fixation	11%
Cross-site request forgery	11%
Insufficient authentication	10%
HTTP response splitting	9%

Cross-site scripting, SQL injection, and most of the others are issues that must be handled by the developers of the software. The Apache and Drupal organizations both have security teams that do so, and the system will be patched on a regular basis. Because there is a service contract, patches will be applied as a matter of course without any involvement needed by the City.

Information leakage problems, however, may be due to web site configuration. Directories are left open for anyone to browse and files are left available to the public instead of locked behind security checks.

Top Ten Hacker Goals

The Web Application Security Consortium (WASC) maintains a Web Hacking Incident Database (WHID) that records major hacking incidents and how they occurred. In a 2008 report (PDF), Breach Security summarized this data into a top ten list of the apparent hacker goals:

⁵ Drawn from "Drupal and Apache Web Site Security Checklist" www.nadeausoftware.com

Goal	%
Defacement	24%
Stealing sensitive information	19%
Planting malware	16%
Monetary loss	13%
Downtime	8%
Phishing	5%
Deceit	2%
Worm	1%
Link spam	1%
Information warfare	1%

Web masters sometimes argue that security isn't that important because they've got nothing worth stealing. But note that the top attack goal is simply to deface the site. If we add together percentages for defacement, planting malware, phishing, deceit, and link spam, then 48% of hacker goals just involve posting bad content to the site. This can put visitors at risk with malware and damage the City's reputation.

Web masters for small sites might also argue that they are too small to be noticed. Automated attack tools, however, don't care if the site is big or small. They simply scan through IP addresses looking for vulnerabilities they can use. The Internet Storm Center collects statistics on the length of time between automated attacks for an average target IP address. The answer: 6 minutes.

Basic Apache Settings

Restrict files listed

WASC classifies file listing problems as a Directory Indexing threat, and one of several types of Information Disclosure issues. WASC's threat classification group has further information on Directory Indexing and other threats.

Disable Apache's directory listings

Apache's mod_autoindex module creates directory listings for any directory without an "index.html" or equivalent. This is sometimes enabled by default in "easy" configurations for beginning users. When enabled, though, it allows hackers to see parts of the site they shouldn't.

Restrict Drupal's file upload lists

By default, Drupal shows a list of a nodes uploaded files at the bottom of the node's page. Unless certain that every uploaded file is suitable for publication, limit or block these automatic file lists

Beware Drupal file manager-style modules

We will check carefully (and probably avoid) any module that can list files on the server.

Restrict the files PHP scripts can access

By default, PHP scripts like Drupal can access any file anywhere on the server, including files outside of the directories served. To limit the damage that a malicious or hacked script can do, file system access from PHP will be limited.

Limit PHP file access to specific directories

PHP's "open_basedir" directive limits PHP scripts to only access files in a list of allowed directories. We will set this to the site's top-level directory, plus the temporary file directory only.

Restrict the types of files served

Drupal distributions include a lot of internal files that don't need to be served. Most of these are innocuous. Others can reveal information about the site to hackers. It isn't practical to restrict access to these files one-by-one. Instead, we will restrict access to whole groups of files based upon their file type.

WASC classifies problems that reveal information they shouldn't as Information Leakage threats. White Hat Security found that information leakage problems were the 3rd hardest to fix — perhaps due to the difficulty of finding the holes the information is leaking through.

Block Apache from serving hidden files

By default, every file in the site's directories can be served. Some clearly shouldn't be, such as Apache's ".htaccess" and ".htpassword" files. In fact, no Linux or Mac OS X file with a name starting with "." should be served.

Restrict Apache to only serve files with safe file types

Served directories can become cluttered with files that shouldn't be served, such as temp files, backups, shell scripts, text file notes, and more. Drupal's modules also often include ".info", ".install", ".inc", and ".module" files that shouldn't be served directly. To avoid serving files that shouldn't be, we will block everything by default, then unblock files with known safe extensions, such as:

Basics	Images	Multimedia	Archives	Documents
.css	.gif	.f4a	.gz	.doc
.htm	.ico	.f4b	.rar	.docx
.html	.jpeg	.f4p	.sit	.odf
.js	.jpg	.f4v	.tar	.ppt
.pdf	.png	.flac	.zip	.pptx
.txt		.flv		.xls
.xml		.mov		.xlsx
.xsl		.mp3		
		.qt		
		.swf		

Restrict Drupal file uploads to only accept files with safe file types

Drupal's core upload module allows files to be uploaded and attached to nodes. If left unrestricted, malicious users can upload viruses and inappropriate or illegal content. Restrict uploaded files to file types in the same safe content list allowed in Apache (see above).

Restrict the context in which files are served

Apache serves any file that passes all allow/deny tests. However, some files, such as images, CSS, and JavaScript, are only relevant when used by one of our own web pages. There are two problems:

- Bandwidth thieves can take advantage of the site by referencing images or scripts from their pages. They get fast downloads and low bandwidth costs because the images come from our site, not theirs.
- Hackers can probe the site and look for specific files to determine what software we're running. For example, sites with "http://YOURSITE.com/misc/druplicon.png" run Drupal.

Both of these problems can be reduced by using Apache's mod_rewrite module to reject requests for images, CSS, and Javascript unless the request has a "referer" URL for a page at the site.

Restrict the PHP scripts executed

While there are many PHP files in Drupal, the following are the only ones ever executed directly via a URL. All other PHP files are loaded by these scripts or by the scripts that they call.

- "cron.php" is invoked regularly to do search indexing and other scheduled jobs.
- "index.php" serves almost everything.
- "install.php" is used during site installation to set up database tables.
- "update.php" is used after adding or updating a module.
- "xmlrpc.php" is used for AJAX callbacks to Drupal.

At a Drupal site, there is normally no need for Apache to run any PHP script other than one of these. So, we will block execution of all PHP scripts generically (see the previous section on file type blocking), then explicitly allow only these PHP scripts under appropriate circumstances.

- Because Drupal is a standard product, the names and locations of its PHP scripts are well-known and easily checked by hacker scripts. WASC classifies problems involving well-known files as Predictable Resource Location threats. White Hat Security, in their Spring 2009 report, estimated that 14% of web sites are likely to have problems of this type.

Allow access to Drupal's "cron.php" from trusted hosts only

For Drupal to work properly, a cron job runs "cron.php" regularly. Typically that job is run by the same host that runs Apache. So access to "cron.php" will be for our host only.

Allow access to Drupal's "install.php" and "update.php" from trusted hosts only

The "install.php" and "update.php" scripts should be runnable from certain specified hosts.

Redirect access to unallowed Drupal files to 404 "Not Found" errors

The above configuration settings ensure that unallowed PHP scripts will not be executed. Attempts to access them return a 403 "Forbidden" error. However, a 403 error still tells hackers that the file exists. We will use Apache's mod_rewrite module to return a 404 "Not found" error instead. The above configuration will be kept as a fail safe.

Reducing Information That can Help Hackers

In a [2009 report](#) (PDF), [White Hat Security](#) reports the top ten vulnerabilities in sites they tested. Number two, with a 47% likelihood, is [Information Leakage](#). Vulnerabilities of this type come in many forms. They needn't just include obvious problems, like posting credit card and social security numbers to public pages. Other information leakage problems reveal information about the site's software and configuration, such as the model and version number of the software, host names, IP addresses, logins, and passwords.

Web masters often rely on "security through obscurity" — hoping that hackers won't notice security flaws. But today's hackers have automated attack tools that scan sites for vulnerabilities, poking at everything in the hope of finding a weakness to exploit. Relying on obscurity is not sufficient.

Reduce published software names and version numbers

Don't tell hackers anything we don't have to. We will disable everything that reveals the software we are using, its version numbers, and its configuration. This will minimize Apache server information in HTTP messages.

Disable or restrict Apache server information pages

Apache's [mod_info](#) module can display a page listing the server's full configuration.

Restrict Apache server status pages

Apache's [mod_status](#) module can display a page listing all the running instances of the server and what they are doing right now. These will be disabled too.

Disable PHP information in HTTP messages

By default, PHP contributes its name and version number to Apache's "Server" field in every HTTP response. It also adds an "X-Powered-By" field and again includes the PHP version number.

Disable the Apache server signature

By default, Apache includes information about the server and web master in its error pages.

Change the default name of the PHP session cookie

PHP provides built-in management of a session cookie. This is used by Drupal, and a lot of other PHP code. Unless set explicitly, the cookie name is "PHPSESSID". Avoid advertising that we're using PHP by changing the default name to something generic

Remove pages that display "phpinfo()"

PHP's "phpinfo" function shows detailed information about the PHP configuration. We never display this output on a public page. Many public sites have this information published.

Remove content that shouldn't be served

Default distributions of Apache and Drupal include files there is no need to serve. When served, they can tell hackers exactly what software and versions are being used.

Block Apache from serving its manual

Apache distributions include full documentation and an "extra/httpd-manual.conf" file that places that manual on-line at "http://YOURSITE/manual".

Move Drupal's text files

Drupal's installation includes helpful text files in the top-level directory, such as "INSTALL.txt", "UPGRADE.txt", and "CHANGELOG.txt". By default, all of these files are served at "http://YOURSITE/INSTALL.txt" et al.

Move Drupal's script files

Drupal's top-level "scripts" directory contains optional shell and perl scripts that help clean up code or run Drupal's "cron.php" automatically. These scripts should never be served. The entire directory will be moved to an unserved directory and the name changed.

Move Drupal's "install.php"

Drupal's "install.php" in the top-level directory is used once during the installation of Drupal. It is never used again, so there is no need to keep serving it.

Remove extra entries from Drupal's "robots.txt"

Drupal's "robots.txt" file requests that search engines skip indexing certain files and directories. After we have moved the above text files and scripts out of the Drupal site directory, we will remove lines for them from "robots.txt". There is no need to advertise that the files ever existed.

Remove Drupal's version number from "robots.txt"

Drupal provides a "robots.txt" file for the site's top level directory. The first line of the file includes a revision control system comment and version number. We will remove it.

Remove Drupal's version numbers in CSS files or enable CSS aggregation

Most of Drupal's CSS files include a revision control system comment that gives a version number. We will remove it

Remove Drupal's version numbers in Javascript files or enable CSS aggregation

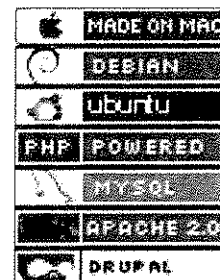
Like Drupal's CSS files, Drupal's Javascript files also include a revision control system comment on the first line. Removed as well.

Remove content that announces what software we use

While we can't remove all evidence of what server-side software we're using, it is possible be less obvious about it.

Remove "badge" images and configuration bragging

Image badges that declare loyalty to Drupal/MySQL/PHP/Apache/Linux/Mac OS X tell hackers how to attack. Remove the badges and any posts that brag about the site's server configuration.



Use a custom favicon instead of Drupal's favicon

Drupal's default configuration provides its own blue-water-drop favicon. Instead of advertising on every page that we are using Drupal, Brisbane will have its own

favicon.

Disable error and debugging information

Avoid advertising software bugs and the inner workings of the site. Block error and debug messages.

Disable PHP on-page errors

By default, PHP errors print messages onto the web pages returned to users. Errors will be written to the site's log

Disable Drupal's on-page errors

By default, Drupal errors are reported to Drupal's log **and** printed onto the offending web page.

Disable Drupal's devel module

Before the site goes into production, we will remove the module

Disable Apache TRACE responses

The HTTP TRACE request is a debug feature that echos back to the sender whatever was sent to the server, including cookies. It can be used by browser Javascripts to bypass browser security and access cookies, including authentication credentials.

Drupal configuration changes that limit who can post content to the site and who can view it

Lock down Drupal accounts

Control how users create Drupal accounts, and what they can do with them.

- WASC classifies account problems as Insufficient Authentication weaknesses. In a 2009 report (PDF), White Hat Security's top ten security issues includes this threat as number nine with a 10% likelihood amongst web sites they tested.

Disable Drupal's anonymous user account creation

By default, Drupal enables anonymous users to create a new account without asking first. A strategy for account creation will be devised.

Block logins to generic Drupal accounts

Web sites have lots of pages that don't need to be owned by any specific user, such as the site's home page, terms of use, or privacy policy. Some sites create a dummy account like "staff" or "general" to own these pages so that they aren't owned by the web master account. It's a bit cleaner that way, but after development these accounts are disabled.

Create Drupal user roles

Drupal user roles give a name to a group of permissions for viewing and creating content and administering the site. By default, there are only "anonymous user" and "authenticated user" roles. This doesn't provide much granularity for controlling access. Roles could be: an "author" role for users that can create and edit content, a "moderator" role for users that can approve comments and delete offending content, and an "administrator" role for users that can make limited changes to the site's configuration.

Assign users their user roles

With user roles created, each of the user accounts will have its role

Set Drupal user role permissions

A role will not get a permission unless the user role needs it.

Set up SSL for Drupal logins

The site will be set up to log in via SSL

Restrict the content users can create

Drupal content can include HTML text, forms, styles, scripts, and even executable PHP code. For web masters, this is very flexible. It can also be very dangerous.

- PHP code in content is executed on the server where it has access to everything. Malicious code could destroy the site. So, block all users except the web master from creating content with embedded PHP code.
- HTML could include scripts executed in the users' browser where they have access to site cookies. Malicious code could send private cookie data elsewhere and make a mess of the site. Block all users except the web master from creating content with embedded scripts.

HTML could include styles, iframes, forms, and images that present foreign content as part of the site, or that simply make a mess of styling.

Create a safe filtered input format for Drupal's anonymous users

Drupal's default "Filtered HTML" input format restricts content to basic paragraph, list, and formatting tags. Avoid abusable tags like <script> <style> <iframe> <form> and <object>. Allowed tags:

<a> <bdo> <blockquote>
 <code> <dd> <dl> <dt> <i>
 <p> <pre> <sub> <sup> <tt>

Create a safe filtered input format for Drupal's trusted users

Drupal's default "Full HTML" input format allows anything, including <script> <iframe> <form> and <object>. That's too much, even for trusted users. Allowed:

<a> <abbr> <acronym> <address> <area> <base> <bdo> <big>
<blockquote>
 <caption> <cite> <code> <col> <colgroup> <dd> <dfn>
<div> <dl> <dt> <h1> <h2> <h3> <h4> <h5> <h6> <hr> <i>
<legend> <map> <p> <pre> <q> <samp> <small>
<style> <sub> <sup> <table> <td> <tfoot> <th> <thead> <tr> <tt> <var>

Restrict access to Drupal's unfiltered input formats

Full HTML format available to the web master only. PHP format disabled.

Install a spam filter module in Drupal

Spam filters use heuristics to decide if content is or is not spam. Content that looks spam-y is redirected to an approval queue where a moderator must decide what to do. A module will be used to filter spam.

Restrict access to PHP code fields

WASC classifies code creation problems as Insufficient Authorization and Application Misconfiguration weaknesses. Of course, once bad PHP code has been inserted, that code can create all sorts of additional problems.

Restrict the nodes listed

Most Drupal sites have internal content that shouldn't be listed or viewed. Some internal content is private, such as a web master's to-do list or security notes on problem users. Some internal content isn't ready for publication yet, such as nodes or comments waiting in a moderator queue. And some internal content is an artifact of site structure, such as the site's "Page not found" and "Access denied" error pages.

WASC classifies content listing problems as a Directory Indexing weakness.

Restrict views to only show published nodes

Drupal's Views module creates lists of nodes meeting filter criteria. The first filter in every Drupal public view should be to only list published nodes. Edit views on the Administer > Site building > Views page.

Restrict views to only show non-administrative nodes

Check all of the views to include a filter to exclude content of that type from public lists of nodes. We will override Drupal's default views, such as "frontpage", "popular_alltime", "popular_recent", and "tracker".

Restrict access to administrator views

Web masters may use their own administrator views to list unpublished content, security notes, and more. Restrict access by setting the user roles that may access a view on each view listed on the Administer > Site building > Views page. Be sure to disable the "access all views" permission for all user roles on the Administer > User management > Access controls page too, or view-specific user roles will be ignored.

Block listing administrative vocabularies in the public site map

Drupal's Site Map module is a handy way to automatically maintain a public site map. By default, it lists all vocabularies and terms. However, some vocabularies may be an artifact of site structure and others may be for administrative use only. These vocabularies and terms should not be listed publically, so configure the module to skip them using the Administer > Site configuration > Site map page.

Block listing administrative vocabularies in taxonomy views

Drupal's default "taxonomy_term" and "taxonomy_directory" views can list any vocabulary and its terms. We will add view filters to exclude administrative vocabularies.

Restrict the nodes indexed and shown in a search

Search is an essential feature for most web sites. Configure it to only index and display appropriate content.

WASC classifies search problems that reveal content they shouldn't as Insecure Indexing weaknesses.

Block listing administrative nodes in the XML site map

Site Map creates an XML site map that lists all site content for easier access by search engines. By default, it lists every published node. However, some nodes are artifacts of site structure or contain administrative content. Search engines don't need to look at these.

Restrict access via Drupal search

Drupal's built-in search features index everything — every published node for every content type. While administrative nodes will not be shown to users unless their user roles allow access, some nodes must be public, and yet shouldn't be listed. For instance, "Access denied" and "Page not found" nodes have to be publically accessible, but they should never show up in a search results list.

Restrict the content users can view

Some site content is intended strictly for the web master, or for managers, authors, moderators, etc. Drupal's user roles restrict specific actions, but not specific content. For that we need to adjust settings and add modules.

WASC classifies content view problems as a type of Insufficient Authorization weakness.

Restrict access to specific Drupal nodes and content types

With additional modules, if needed.

Restrict access to specific Drupal menus

Individual menu blocks can be restricted using user role restrictions

Restrict access to specific Drupal blocks

Hide private blocks by setting block permissions on each block

City of Brisbane
Public Information Subcommittee
Agenda Report

TO: City Council via City Manager
FROM: Administrative Management Analyst
DATE: Meeting of December 22, 2009
SUBJECT: Web Developer Recommendation

City Council Goals:

To develop management and fiscal systems to maximize effectiveness of city services and accountability to Brisbane taxpayers and citizens. (11)

To encourage community involvement and participation. (15)

Purpose:

Present the Subcommittee with a recommendation for a new web developer to re-design the City's website.

Recommendation:

For the Subcommittee to give direction to move forward with staff's recommendation.

Background:

The Public Information Subcommittee met on June 9th to discuss key criteria for the City's new website. From the various criteria which were discussed, the following key criteria were identified:

- Key Criteria #1: Secure Performance
- Key Criteria #2: Easy to Navigate
- Key Criteria #3: Greater Visibility of the Things Citizens are Interested In
- Key Criteria #4: Ease of Updating and Viewing Information

From the list, Secure Performance was deemed to be the most important. Beginning last Spring, the City website had been the victim of multiple SQL injection attacks, which rendered some of the pages unreadable or completely blank in some instances.

During the June 9th meeting, the Subcommittee also identified they would like to extend a Request for Proposals (RFP) to local web developers. This would allow for quick changes and updates to be made whenever necessary, as well as ensure the website was unique to Brisbane, offering visitors a more “local” look and feel.

An RFP was sent to a dozen web developers in town, identified through a search of current business licenses on file with the City, and those whom staff knew to be adept in web design and development.

Two applicants submitted proposals to the City by the due date (September 25, 2009), from Brisbane residents C.J. MacDonald and Alison Wilson.

An ad hoc Website Redesign Committee was soon convened to review the two RFPs and make recommendations based on the key criteria specified by the Subcommittee. This Web Redesign Committee was made up of Albert Duro, IT Manager; Betsy Cooper, Financial Services Manager; Sheri Spediacci, City Clerk and Webmaster, Wilma Kwan, MTEP representative and Technology Librarian for the City of San Bruno, and Caroline Cheng, Administrative Management Analyst.

Discussion:

With C.J.’s application being over five times the length of Alison’s, it became apparent to the Committee as they went through it that much more attention was given to addressing the Subcommittee’s four key criteria. Most importantly, C.J.’s mention of Drupal, the content management platform he would use to build the new website with, would be highly proficient in providing the City with a secure technology, being a “well-known system in use on thousands of websites and watched by thousands of developers.” Also, what is unique about Drupal is that it’s “open source” software, meaning, all the web developers who use Drupal have their eyes on the code, watching for any vulnerabilities. Whenever a problem with the code is noticed, it’s able to be quickly identified and patched. This is the main problem with our current website developer, e21, where, due to poorly written code, SQL injection attacks were able to occur unnoticed. It wasn’t until staff came across the unreadable or blank pages that e21 also became aware of the problem. By that time, it was too late to correct for all the poorly-written code, with SQL injection attacks currently unavoidable whenever the website is “unlocked” by a Web Administrator in order for it to be updated with new information by staff.

In addition, C.J. provided many examples of past work experiences implementing the Subcommittee-identified key criteria on other client websites, and how Drupal was very effective as an open source content management system (CMS). He also provided many suggestions beyond what was specified in the RFP, such as the CMS being hosted on a Virtual Private Server (VPS). This would allow for high performance, good security, and good administration. The host which C.J. suggested, vps.net, provides security audit

services which serves as another set of eyes. The Website Redesign Committee felt that this hosting provider would be highly advantageous for the City to have. In addition, C.J. has worked closely with the system before and noted how it is highly scalable to accommodate the different features and criteria the Subcommittee would like to see reflected on the City's new website.

The Website Redesign Committee invited both applicants to come in to City Hall in mid-October to present them with a demonstration of what they envisioned the City's new website to look like. C.J. showed the ease of using Drupal by logging in to the back-end administration of one of the sites he manages, www.cinegogo.net, so staff could see what it looks like to update the calendar with a new event and how it automatically will self-populates to the homepage, making content generation and maintenance smoother and simpler than it is.

Although the pricing estimate indicated in C.J.'s proposal is higher than Alison's cost, \$48,200 vs. approximately \$30,000, the Website Redesign Subcommittee felt there were grounds for recommending C.J. Most notably, ongoing maintenance costs and software acquisition and upgrades would close the \$18,200 gap. Drupal is open source software and is free to begin using, whereas Alison is recommending using Adobe Dreamweaver to build the new website with. Licensing for Adobe software is expensive, and given the number of Web Administrators we have currently, acquiring the software would alone be a steep cost. Also, C.J. specified eight hours per month for website maintenance in the service contract, which could be rolled over to the next month if not completely used in the current month. Any additional maintenance or training would be \$85 per hour. Alison specified only "train the trainer" costs (for Adobe Dreamweaver) to be \$75 to \$125 per hour or a negotiated flat rate.

Fiscal Impact:

None, due to the City having received a federal technology grant in December 2008 where up to \$50,000 can be utilized for a new website.

Measure of Success:

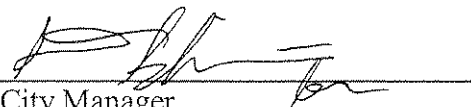
A secure, easily-navigable website for the City that is able to better interact with and serve the Brisbane community.

Attachments:

- A – Alison's proposal
- B – C.J.'s proposal



Administrative Mgmt. Analyst



City Manager

City of Brisbane
Agenda Report

TO: Honorable Mayor and City Council

FROM: Caroline Cheng via Clay Holstine, City Manager

DATE: Meeting of January 12, 2010

SUBJECT: Maintenance Costs for the Current and Proposed City Website

PURPOSE: Review the maintenance costs staff determined for the City's current website and those which the recommended web developer determined for a new website.

RECOMMENDATION: Review and comment on the prepared monthly and annual costs.

BACKGROUND:

On December 15, 2009, the Public Information Council Subcommittee met to review staff's recommendation for a new web developer who will be redesigning the City's website. The process of doing so began last June 2009, when the City was awarded \$50,000 in Federal funds which could be used towards website improvements and upgrades.

The recommended web developer was chosen based on his thorough proposal which highlighted each of the Subcommittee's four key criteria for the new website (secure performance, easy to navigate, greater visibility of the things citizens are interested in, and ease of updating and viewing information). He showed this in his proposal through previous websites he had developed, as well as in his demonstration to the City's ad hoc Website Redesign Committee of how the website would be maintained.

At their December 15th meeting, the Council Subcommittee requested staff to obtain cost information for the City maintaining its current website, as well as indicate what it would cost the City on a monthly basis should they proceed with selecting the recommended web developer for the City's website redesign. In addition, clarification was requested in regards to staff training and what additional costs, if any, would be needed in order to maintain the new website.

DISCUSSION:

Albert Duro, IT Manager for the City, estimated the monthly cost for maintaining the City's current website to be \$658.33. This was broken down into four components: Server hardware (\$62.50), Accessories & miscellaneous (\$20.83), Server software (\$75.00), and Administration (\$500.00). Thus, the annual cost for maintaining the website would be \$7,900.

In his original pricing estimate, C.J. had indicated total monthly charges to be \$787.08, which included a monthly maintenance charge of \$420.00. The type of maintenance this amount would cover would be: monitoring, making any necessary patches, as well as any minor upgrades. C.J. has since determined that 3.25 hours of monthly maintenance would be enough to cover these tasks, at an hourly billing of \$85.00. Thus, the \$420.00 amount would be reduced to \$276.25. Combined with the cost for hosting, backups, and security as originally estimated (\$367.08), C.J.'s total monthly cost would be \$643.33, for an annual charge of \$7,719.96.

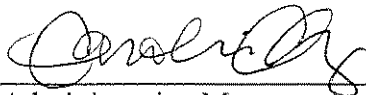
In regards to training staff on how to maintain the new website, C.J. had included an amount of \$3,000 for training. Since C.J.'s billing rate is \$85/hr., the total hours available for training would be 35.3. When asked how those hours would be broken down, C.J. indicated that five 2-hr. sessions would be for group training on how to use Drupal. This would include adding content, updating pages, learning the user interface, and getting familiar with permissions and security best practices. Secondly, he suggested the following one-on-one training: 8 hours for Caroline (for setup and training with blogging possibly other social networking tools); 8 hours for Albert (for infrastructure and systems with the hosting provider), and 5 hours for Sheri (for document management). That leaves 4.3 hours which would be available should more training be needed. C.J. does not believe the total training will surpass the 35.3 hours or \$3,000 amount.

FISCAL IMPACT/FINANCING ISSUES:

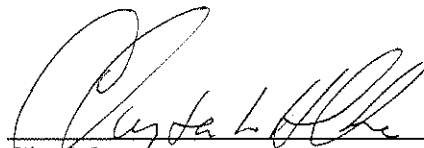
The \$50,000 grant would cover C.J.'s one time costs of \$48,200. After the website is set up, annual costs would be \$7,719.96.

MEASURE OF SUCCESS:

A secure, easily-navigable website for the City that is able to better interact with and serve the Brisbane community.



Administrative Management Analyst



City Manager

ATTACHMENTS:

A – Pricing Estimate (p.11-12) of C.J.'s original proposal